E-Briefings

Volume 16, No. 5 • September 2019

New research and expert opinions in
the area of hospital and health
system governance.

Cyber Risk Management: A Business Enabler (Not an IT Issue)

By Bob Chaput, Executive Chairman and Founder, Clearwater

Cyber risk management (CRM) is not an "IT problem"; it is an enterprise risk management matter that can be harnessed into a business enabler. The healthcare industry is experiencing a time of unprecedented change, including ongoing digital transformation. We must simultaneously undergo a CRM transformation.

Healthcare continues to be the single most-targeted industry for cyberattacks[1]—and your organization might be next (if you haven't been attacked already). The consequences of cyberattacks on hospitals and health systems can be far-reaching. Patient lives may be at risk, for example, when a ransomware attack disrupts the availability of data and a provider is unable to deliver services. An organization's finances and reputation can be put at risk as well. Violations of the privacy and security requirements spelled out in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) can result in fines, penalties, and corrective actions being levied against the organization. And more recently, litigation related to data breach incidents has demonstrated an increased risk of personal liability for an organization's directors and officers.

Key Board Takeaways

The first step in addressing cyber risk is engaging in a conversation about what cyber risks exist, the potential impacts on your organization, and steps that can be taken to strengthen the CRM program. Following are some key discussion questions to get you started:

1. Have you discussed *fiduciary responsibility, duty of care*, and *reasonable diligence* with respect to managing cyber risk?
2. In the event of a successful cyberattack on your organization, how prepared is the CEO to address concerns from internal and external stakeholders, with strong, unequivocal messaging about the CRM program?
3. Is your current approach to CRM well-aligned with the organization's vision, mission, values, and services?
4. Is your organization likely to be involved in any M&A activity in the next several years? Would your approach to CRM pass the due diligence process?
5. Is your organization prepared to go toe-to-toe with healthcare industry disruptors with respect to its ability to protect data from cyber risks?

Personal Liability

In the 1996 *Caremark* decision, the Delaware Chancery Court declared that, in such actions, directors can be held personally liable for failing to "appropriately monitor and supervise the enterprise."[2] Recent data breach litigation shows how corporate executives and board members can be at risk of personal liability when a cybersecurity incident occurs.

Derivative litigation was also brought against Yahoo, Inc. for data breaches that occurred in 2014 and 2016. The $29 million settlement, approved in January 2019, "represents the first significant recovery in a data breach-related derivative lawsuit targeting directors and officers for breach of fiduciary duty."[3] The litigation that followed the 2017 Equifax, Inc. data breach also named certain officers and directors of the organization.[4]

HIPAA is the foundational legislation for the data security and privacy requirements that apply to any

[1] *Managing Enterprise Risks in a Digital World: Privacy, Cybersecurity, and Compliance Collide*, 2019 Data Security Incident Response Report, BakerHostetler.

[2] Brenda Sharton and Gerard Stegmaier, "Breaches in the Boardroom: What Directors and Officers Can Do to Reduce the Risk of Personal Liability for Data Security Breaches," Thomson Reuters, 2015.

[3] Freya K. Bowen, "Recent Developments in Yahoo and Equifax Data Breach Litigation Suggest Increased Risk of Personal Liability for Directors and Officers for Cybersecurity Incidents," Perkins Coie Tech Risk Report, February 6, 2019.

[4] *Ibid.*

The healthcare industry is experiencing a time of unprecedented change, including ongoing digital transformation.

entity that "creates, receives, maintains, or transmits protected health information."[5] HIPAA's language sets expectations of organizations with definitions of *reasonable cause, willful neglect, and reasonable diligence*, which refers to the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.[6] The Office for Civil Rights (OCR) uses these definitions to evaluate the scope of responsibility the organization holds for lack of compliance with regulatory requirements and civil money penalties.

In the event of a cybersecurity incident or data breach, the courts and OCR want to know the same thing: did your organization do everything, within reason, that it could to prevent the incident from happening? Or did your organization demonstrate "negligence" or "willful neglect" with respect to your CRM responsibilities?

It is the role of executive leadership and the board, not IT, to provide informed direction and oversight for the organization's CRM approach, activities, and strategy.

The Shift to Leveraging CRM as a Business Enabler

Hospitals and health systems are facing especially challenging times. Profit margins are shrinking as costs rise. Legislation, policies, and regulations are changing fast. Non-traditional organizations, like Apple and Google, are positioning themselves as industry disruptors, eager to claim a share of the $6 trillion in annual healthcare spending projected to take place in the U.S. by 2027.[7] Following are just two examples of leveraging CRM to meet these challenges.

Facilitating M&A Activity

A survey by Definitive Healthcare identified consolidation as the most important trend impacting the healthcare industry in 2019.[8] What role does CRM have to play in mergers and acquisitions (M&A)? A lot, it turns out. One of the drivers of healthcare M&A activity is "using data more effectively to improve quality and outcomes, such as through personalized medicine or interoperable data exchange."[9]

A global survey of M&A professionals by the Merrill Corporation found that "data privacy" concerns were among the most likely factors to sink a healthcare M&A deal, right after "political uncertainty" and "investor confidence."[10]

Regardless of whether your organization is primed to acquire another organization or to be acquired, it is critical to build M&A considerations into your CRM program.

Competing with Disruptors

In its 2018 report on healthcare industry disruption, Pricewaterhouse Coopers (PwC) identified "technology invaders" shaking up the industry.[11] PwC describes technology invaders as "technology companies seeking to grab a greater foothold in healthcare."[12] Apple is one example with its Health app.[13] Other examples include Google and Amazon. As global players, they also bring mature CRM experience and resources to the table to meet stringent compliance, data privacy, and security and risk management standards from around the world. What this information points out is that all healthcare organizations—whether traditional or disruptive—need to pay attention to data privacy, security, and CRM issues to be competitive.

[5] 45 CFR § 160.103

[6] 45 CFR § 160.401

[7] "National Health Expenditure Projections 2018–2027, Forecast Summary," Centers for Medicare & Medicaid Services, 2019.

[8] "Definitive Healthcare Releases Results of 2019 Annual Healthcare Trends Survey" (press release), Definitive Healthcare, April 22, 2019.

[9] Keith Anderson, Robert Belfort, and Fatema Zanzi, "Mapping the Healthcare M&A Landscape," Manatt, Phelps & Phillips, LLP, March 22, 2019.

[10] "M&A Professionals Bullish on Healthcare Deals for Next Year, Despite Political Uncertainty Concerns: Merrill Insight™ Poll," Merrill Corporation, May 22, 2019.

[11] *The New Health Economy in the Age of Disruption*, PwC Health Research Institute, April 2018.

[12] *Ibid.*

[13] "Institutions That Support Health Records on iPhone and iPod Touch (Beta)," Apple.com, August 19, 2019.

The Governance Institute thanks Bob Chaput, Executive Chairman and Founder, Clearwater, for contributing this article. He can be reached at bob.chaput@clearwatercompliance.com or (615) 496-4891.